National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CGS Architecture Reviews Capability

Version 1.1.1

The Architecture Reviews Capability establishes Architecture Reviews, which are requirements-based reviews to determine whether the requirements were satisfied by the architecture. Security Architecture Reviews focus specifically on determining whether the security requirements for a system, application, or service were included in the architecture (sometimes called security architecture). The reviews demonstrate security requirement satisfaction as well as potential vulnerabilities as a result of missing requirements. The review may be conducted on logical or physical architectures.

07/30/2012

CGS Architecture Reviews Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

The Architecture Reviews Capability establishes Architecture Reviews, which are requirements-based reviews to determine whether the requirements were satisfied by the architecture. Security Architecture Reviews focus specifically on determining whether the security requirements for a system, application, or service were included in the architecture (sometimes called security architecture). The reviews demonstrate security requirement satisfaction as well as potential vulnerabilities as a result of missing requirements. The review may be conducted on logical (e.g., data flows) or physical (e.g., physical connections) architectures.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Security architecture is a high-level depiction of how the security requirements are going to be met and is demonstrated through the traceability of the requirements. The Architecture Reviews Capability evaluates met and unmet security requirements and is conducted during development and integration as well as during the operational phase of the system development lifecycle (SDLC).

An understanding of the mission that the architecture is supporting is essential in finding any gaps in the security requirements traceability. The Understand Mission Flows Capability provides this mission information to the security architect (or architect reviewer) to help determine whether the architecture accurately reflects the requirements and whether the right set of requirements has been developed for the architecture. For integration into other architectures, mission information is also key to understanding and outlining the relationships between the connecting enclaves to determine whether additional requirements need to be included. This understanding is

provided by the Understand Data Flows, Network Boundary and Interfaces, and Network Boundary Protection Capabilities.

Architecture Reviews shall also determine alignment with Enterprise architectures. Conforming to Enterprise architectures enables the reuse of security services as well as centralized security management. Both principles help to ensure that approved security solutions are employed and use of these services reflected in the system design. These types of reviews also ensure consistency between lower-level architectures and architectures at the Enterprise level. Lower-level architectures shall be consistent with the system engineering language used with higher-level architectures.

All Architecture Reviews shall be performed by dedicated security engineers, employed either internally or externally. An external Architecture Review shall be performed when an Enterprise does not have the manpower or expertise to conduct a security Architecture Review. In some cases, an independent review shall be required. An external security engineer shall be used to conduct this type of review. Because of conflict of interest, designers and/or integrators shall not be designated to review the security architecture.

Logical security Architecture Reviews are developed based on an abstract model of the target system, application, or service. The review examines the functional decomposition of the functionality driven by the Security Requirement Traceability Matrix (SRTM). The reviewer considers the risk posture when determining the strength and adequacy of mechanisms to determine whether any requirements are not present which shall be included. This abstract model is used to understand the functions that shall be performed and secured. It shall determine whether the architecture supports the services (requirements) that were defined. This review helps to determine whether the strength of security mechanisms, controls, interfaces, and information assurance (IA) concepts (e.g., confidentiality, integrity, availability, authentication, and non-repudiation) are adequate.

Physical security Architecture Reviews shall examine the physical architecture, which is the beginning of the realization of the design. This review evaluates the physical components, connections, and their functionality against their allocated requirements. The security engineer shall be able to determine whether a component has security functionality allocated to it based on the decomposition of requirements in the SRTM in the security architecture. As with logical security Architecture Reviews, physical reviews provide insight as to whether the physical security architecture meets the requirements

and whether all of the right requirements have been defined and documented for the architecture.

The Architecture Reviews Capability shall establish Architecture Reviews as part of the Enterprise's milestone reviews through the system development phases (e.g., Preliminary Design Review [PDR] and Critical Design Review [CDR]). For the development phase, systems Architecture Reviews shall be performed in a timely manner such that they can influence the system design, rather than finding architecture flaws after the Design Phase has been completed; therefore, architectures being reviewed shall be scalable and extensible. When integrating an architecture with existing architectures, the reviewer shall ensure that the enclaves, subsystems, and network architectures are compatible and function together in a complete secured system architecture. In addition, the reviewer shall ensure that the security system construct does not violate the architectures' security requirements. Understanding the connections and interface controls links for integration is provided by the Enterprise's network diagram for a visualization of system connectivity (See Network Mapping Capability).

Architecture Review outputs shall be provided to the program security engineer and program manager to ensure that the appropriate changes are made and recommendations for improvements are incorporated for the construct. These identified problems and recommendations shall also be provided to the Development and Risk Mitigation Capabilities.

The Architecture Reviews are also conducted against operational systems, applications, or services. Examining operational systems architectures provides an architectural review of implemented systems, networks, or Enterprise architectures to confirm that requirements are met. Operational reviews are used to identify potential weaknesses, which mean that the requirements are not met within the architecture. To aid in the determination of whether the requirements are met, documentation shall be provided with an architecture model. If documentation is not available, reverse engineering of the architecture model shall take place to provide an analysis of met and unmet requirements (this activity shall be conducted during Network Security Evaluations (see the Network Security Evaluations Capability for additional information).

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Enterprise services are established and known.
2. Boundaries and interfaces are clearly defined.
3. Architectures exist and are documented for systems in both design and operations.
4. The network diagram or system diagram is already present.
5. The risk was understood and taken into account when the architecture was developed.
6. Security requirements are provided.
7. The mission and data flows are understood and documented.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability provides recommendations for use by Risk Mitigation.
2. The Capability reviews comprehensiveness as defined by the material provided.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When the Architecture Review Capability is implemented properly, it will provide the Organization with the functionality to perform extensive reviews of its architectures to find weaknesses in the security architecture through unmet security requirements, covering all legacy threats plus all new threats that are recognized from the review. Enterprise architectures, which require the management of systems of systems, can be very complex or very simple and their weaknesses can likewise be complex or simple. Architecture Reviews are intended to find as many weaknesses as possible in the architecture, whether the weakness is the result of an inherent flaw in the system's

design, improper implementation, or poor configuration. The review process will encompass both physical and logical architectures and be conducted during development and operations.

The Organization will have an understanding of logic behind the security of its system, application, or service that will help in determining the need for additional security mechanisms to meet requirements. The Organization will have this understanding to allow for scalability and extensibility in the architecture to integrate additional security components, as determined by the Architecture Review. These security Architecture Reviews will also identify security components that the system will inherit as well as who has responsibility for those security mechanisms.

An Organization will have an understanding of its risk and risk posture, which is key in identifying issues during the Architectural Review. If the Architecture Review is performed by an external team, the Organization will provide the team with the risk information. Accepted risks may have adverse effects on the Enterprise; therefore, risks culminating from all individual system risks will be expressed and tracked through the agency Enterprise architecture process.

An Organization will be tasked with establishing procedures to conduct an Architecture Review. If the Architecture Reviews are provided internally, the Organization will need to define the Architecture Review process and procedures; if externally, it will review the procedures defined by the external team. Determining how often Architecture Reviews take place will be defined by the Organization, and the frequency of the reviews will depend on the complexity of the networks or systems, the risk of attack, and data protection requirements.

Upon completing Architecture Reviews, a report will be generated for the program security engineer containing all of the outputs and recommendations for the system architecture. The report will be consistent with the system engineering language used to ensure effective communication.

Based on Architecture Reviews, an Organization will determine that all relevant basic security precautions have been followed when securing a network/system, including the Architecture Review-recommended use of anti-malware, software firewalls, cross-domain solutions, user authentication, and demilitarized zones (DMZs).

An Organization will have usage policies as an input factor for Architecture Reviews. In addition to being assessed for security requirements, the usage policies will be assessed for weaknesses. An Architecture Review will evaluate the design situation weaknesses, which may allow users to circumvent security, and find ways to modify policies so the systems are secure while still being user friendly. These findings will be reported to the program security engineer.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Understand Mission Flows–The Architecture Reviews Capability relies on the Understand Mission Flows Capability to provide requirements that are levied on the architecture.
- Understand Data Flows–The Architecture Reviews Capability relies on the Understand Data Flows Capability to provide requirements that are levied on the architecture.
- Development–The Architecture Reviews Capability relies on the Development Capability to ensure that reviews occur during the development phase of the lifecycle to ensure that the architecture meets requirements during system design.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Architecture Reviews Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Architecture Reviews Capability relies on the IA Policies, Procedures, and Standards Capability to provide

information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The Architecture Reviews Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Architecture Reviews Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Architecture Reviews Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Mapping–The Architecture Reviews Capability relies on the Network Mapping Capability to provide visualization of the relationships and connectivity between components that is used when determining security requirements.
- Network Boundary and Interfaces–The Architecture Reviews Capability relies on the Network Boundary and Interfaces Capability to provide system/network information used for understanding the relationships between connecting enclaves when determining security requirements.
- Network Boundary Protection–The Architecture Reviews Capability relies on the Network Boundary Protection Capability to provide system/network information used for understanding the relationships between connecting enclaves when determining security requirements.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	**Related Text**
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
CM-7 *LEAST*	Control: The organization configures the information system to

FUNCTIONALITY	provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services]. Enhancement/s: (1) The organization reviews the information system [Assignment: organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services. (3) The organization ensures compliance with [Assignment: organization-defined registration requirements for ports, protocols, and services].
PL-5 *PRIVACY IMPACT ASSESSMENT*	Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy. Enhancement/s: None Specified.
SA-8 *SECURITY ENGINEERING PRINCIPLES*	Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Enhancement/s: None Specified.
SA-14 *CRITICAL INFORMATION SYSTEM COMPONENTS*	Control: The organization: a. Determines [Assignment: organization-defined list of critical information system components that require re-implementation]
PM-7 *ENTERPRISE ARCHITECTURE*	Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Enhancements: None Specified

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Architecture Reviews Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 501 Discovery and Dissemination or Retrieval of Information Within the Intelligence Community, 21 January 2009, Unclassified	Summary: This directive assigns responsibility to the Intelligence Community (IC) Chief Information Officer (CIO) for developing the information technology (IT) architecture that supports the Office of the Director of National Intelligence.
ICD 503 IC Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008, Classified	Summary: This directive establishes IC policy for IT systems security risk management certification and accreditation. Directs the use of standards for IT risk management established, published, issued, and promulgated by the IC CIO, which may include standards, policies, and guidelines approved by the National Institute of Standards and Technology (NIST) and/or the Committee on National Security Systems (CNSS). IA requirements will be identified and validated through a standard process; therefore, an understanding of the system architecture is necessary to make the appropriate risk decisions.
ODNI/CIO-2009-190 Memorandum, IC CIO Council Decision Regarding the Joint Architecture Reference Model, 7 July 2009, Unclassified	Summary: This memorandum documents decisions by the IC CIO Council including the decision to recognize the Joint Architecture Reference Model (JARM) v1.0.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 4630.05	Summary: This directive establishes policy that IT and

Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), certified as current as of 23 April 2007, Unclassified	National Security Systems (NSS), of the Department of Defense (DoD) Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant IA. The GIG architecture shall be used as the organizing construct for achieving net-centric operations. In addition, it requires IT and NSS interoperability and supportability needs shall be derived using Joint Operating Concepts, Joint Functional Concepts, and associated integrated architectures and shall be updated as necessary throughout the system's life. For IT and NSS supporting DoD business areas and domains, the GIG architecture shall be used to determine interoperability and capability needs.
DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008, Unclassified	Summary: This instruction applies to all defense technology projects and acquisition programs... and it includes Major Automated Information Systems (MAIS). It identifies the DoD Enterprise Architecture, and it shall underpin all information architecture development.
DoDD 8000.01 Management of DoD Information Enterprise, 10 February 2009, Unclassified	Summary: This directive establishes policy that all aspects of the DoD Information Enterprise, including the GIG infrastructure and Enterprise services and solutions, shall be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a DoD net-centric environment. The DoD Enterprise Architecture shall be maintained and applied to guide investment portfolio strategies and decisions to establish and enforce standards and guide security and IA requirements across the DoD. It also sets policy that requires the review of all IT investments for compliance with these architectures and IT standards.
DoDD 8115.01, Information Technology Portfolio Management, 10 October 2005, Unclassified	Summary: This directive establishes policy requiring that all IT investments shall be managed as portfolios to ensure IT investments support the department's vision, mission, and goals; ensure efficient and effective delivery of capabilities to the warfighter; and maximize return on investment to the Enterprise. Each portfolio shall be managed using the GIG architecture.
DoDI 8410.02, NetOps for	Summary: This instruction establishes policy for network

the Global Information Grid (GIG), 19 December 2008, Unclassified	operations (NetOps) and responsibilities for the heads of DoD components to participate in the development of the required operational views for a NetOps Enterprise Architecture.
DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified	Summary: This instruction establishes the DoD Information Assurance Certification and Accreditation Process (DIACAP) for authorizing the operation of DoD information systems. The process manages the implementation of IA capabilities and services and provides visibility of accreditation decisions. As a part of the identification and validation standard process for IA requirements, Architecture Reviews shall be used to validate security requirements across all of DoD and the GIG architectures.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Architecture Reviews Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	

DoD CIO Memorandum, The Department of Defense Architecture Framework (DoDAF) version 2.0, 28 May 2009, Unclassified	Summary: The promulgation memo is the prescribed framework for all department architectures. This version of the framework provides extensive guidance on the development of architectures supporting the adoption and execution of net-centric services within the department (http://cio-nii.defense.gov/policy/eas.shtml).
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Internal versus external–Implementing this Capability internally or outsourcing its functions will change the cost structure.
2. Solution used for implementation–The Enterprise will need to provide tools for operational reviews.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Architecture Reviews Capability.

- The Enterprise shall establish architecture reviews, which are requirements-based to determine whether the requirements were satisfied by the architecture. Security architecture reviews focus specifically on determining whether the security requirements for a system, application, or service were included in the architecture (sometimes called security architecture). The reviews demonstrate security requirement satisfaction as well as potential vulnerabilities as a result of missing requirements. The review may be conducted on logical (e.g., data flows) or physical (e.g., physical connections) architectures.
- The Enterprise shall evaluate met and unmet security requirements during development, integration, and operational phases of the SDLC.
- The security architect (or architect reviewer) shall leverage mission data to help determine whether the architecture accurately reflects the requirements and whether the right set of requirements has been developed for the architecture.
- Architecture reviews shall determine alignment with Enterprise architectures to enable the reuse of security services as well as centralized security management. This ensures that approved security solutions are employed and use of these services is reflected in the system design.
- Architecture reviews shall ensure consistency between lower-level architectures and architectures at the Enterprise level. Lower-level architectures shall be consistent with the system engineering language used with higher-level architectures.

- All architecture reviews shall be performed by dedicated security engineers, employed either internally or externally. Designers and/or integrators shall not be designated to review the security architecture because of conflict of interest.
- An external architecture review shall be performed when an Enterprise does not have the manpower or expertise to conduct a security Architecture Review or when an independent review is required.
- Logical security architecture reviews shall be developed based on an abstract model of the target system, application, or service. The review shall examine the functionality driven by the SRTM.
- The risk posture shall be considered when performing a logical security architecture review to determine the strength and adequacy of security mechanisms, controls, interfaces, and IA concepts and to identity missing requirements.
- Physical security architecture reviews shall examine the physical architecture to evaluate the physical components, connections, and their functionality against their allocated requirements in the SRTM.
- Architecture reviews shall be established as part of the Enterprise's milestone reviews through the system development phases (e.g., PDR and CDR).
- For the development phase, systems architecture reviews shall be performed in a timely manner such that they can influence the system design, rather than finding architecture flaws after the Design Phase has been completed; therefore, architectures being reviewed shall be scalable and extensible.
- When integrating an architecture with existing architectures, the reviewer shall ensure that the enclaves, subsystems, and network architectures are compatible and function together in a complete secured system architecture. The architect reviewer shall ensure that the security system construct does not violate the architectures' security requirements.
- Architecture review outputs shall be provided to the program security engineer and program manager to ensure that the appropriate changes are made and recommendations for improvements are incorporated for the construct.
- The architecture reviews shall be conducted against operational systems, applications, and services to confirm that requirements are met.
- To aid in the determination of whether the requirements are met, documentation shall be provided with an architecture model.